DEPARTMENT OF DEFENSE BLOGGERS ROUNDTABLE BRIEFER: COLONEL WAYNE PARKS, DIRECTOR, COMPUTER NETWORK OPERATIONS PROPONENT, ELECTRONIC WARFARE PROPONENT AND TRADOC CAPABILITIES MANAGER FOR ELECTRONIC WARFARE INTEGRATION AT THE COMBINED ARMS CENTER SUBJECT: INFORMATION AND CYBERSPACE; INFORMATION AS COMBAT POWER MODERATOR: CHARLES "JACK" HOLT, CHIEF, NEW MEDIA OPERATIONS OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE PUBLIC AFFAIRS TIME: 10:30 A.M. EDT DATE: TUESDAY, APRIL 8, 2008

COL. PARKS: Hey, Jack, it's Wayne Parks. How are you doing?

MR. HOLT: Hi, Colonel Parks. We're doing well here. Thank you very much and glad you could join us this morning.

And Colonel Wayne Parks is the director of the Computer Network Operations Proponent and the Electronic Warfare Proponent. He's also the TRADOC Capabilities Manager for Electronic Warfare Integration at the Combined Arms Center out of Fort Leavenworth, Kansas.

A long title there for you, sir. Do you have an opening statement for us? The floor is yours. COL. PARKS: Yes, I do. And one other thing I have been doing for about six months now, Jack, is the interim director for the Information Operations Component.

And here from the Combined Arms Center, there's been a couple of things happened over the last six months with the release of Field Manual 3-0 Operations. And what it has done is it has taken the I/O construct as we have known it, and it's put a different twist on it as we try to operate in and amongst the population, you know, in several places across the world. And what we have had to do is, in Chapter 7 now, which is called "Information Superiority," we've had to put an emphasis on the use of information and how we engage with people with information in a different aspect than you've seen in the past.

So what I want to do today is just try to explain that to you. And then as you heard Jack say, my real job is the computer network operations and electronic warfare aspects of how we're doing business in the Army as well. And there's some nuances to what we've learned in our current operations, to especially electronic warfare, and we'll try to describe some of that for you today and answer whatever questions you might have.

The proposed themes I put out there, let me just run down through those real quick because I think this kind of encapsulates what it is I'd like to portray to you today and then maybe sets it up for some questions you have back to me.

But as I started out, the difference between how we have to operate in the land in what you do in the other domains of air, sea and space is that fact you've got to integrate yourself with the population. And sometimes, you know, lest we forget it in the Army, and certainly not everybody understands it unless you're a Marine or a soldier on the ground. So that's caused us to have to take a look at this thing we're calling information engagement, bringing elements together such as Public Affairs and the Psychological Operations, the Defense support to public diplomacy, combat camera, soldier and leader engagement.

We've had to put a lot of emphasis on looking at how we do that and what's being successful in the theaters now. And then where do we need to go with this in the future to ensure we sustain our capability to operate on the ground in and amongst those populations. And that's caused a little bit of a twist on how we're looking at information operations for the future. So that's what the information engagement is.

Not only are we in that face-to-face business, but certainly, as the technology is available today through computers, networks, electronics and other things along those realm -- you know, that's another place that we obviously interact fairly heavily -- but immediately is is when we're committed and deployed, a lot of that's being done face-to-face. The idea of CNO, computer network operations, and electronic warfare, as we've known it in the past, is obviously changing as well because when you pick up your iPhone today, what you're operating in is a computer network environment at the same time that you're working across the electromagnetic spectrum. And so what we're doing is is taking a look at what's being successful in theater and then doing some experimentation for the future. And what you see turned to cyberelectronic warfare for the future is making sure we understand that environment and how we're going to operate in that environment.

And we're right now at the Combined Arms Center poised as the lead for developing cyberspace and electronic warfare capabilities for the United States Army. And we're partnering with our land component partners, the Marine Corps, as we try to move forward with that.

The next one on full-spectrum operations. You know, the idea of going to combat doesn't really excite any of us, you know. So the idea of maybe preventing war and being prepared to conduct war, when necessary, and then immediately get ourselves in a position to prevent further war is kind of my description of what full-spectrum operations is. And we could be operating in any one of those areas across that spectrum. But we have found for the area of information and cyberspace and electronic warfare or the electronic world, we're certainly doing that across all those spectrums of the operation. And it doesn't stop with one or the other, it's just kind of a level of intensity depending upon what the situation is.

And then lastly is is the one thing that General Caldwell has been adamant about with us is on our joint, interagency, intergovernmental and multi-national integration working with our partners. Sometimes we have a tendency of working with our partners by approving things within the Army and then approving things in the other services and then coming together versus what we're trying to do now is bring the interagency and the Army together at the same time along with our joint services and along with our multi-national partners. So we do this in a collaborative nature versus waiting until everybody gets approval before we start working with each other.

And if that will do, gentlemen, I'll open it up to your questions now.

MR. HOLT: All right, sir. Thank you very much.

We had a couple of folks joined us late. Who is there?

All right, well, we'll get to that here in just a minute.

Steeljaw Scribe, you were first online, so why don't you get us started.

Q Okay, thanks, Jack. And Colonel Parks, thanks for joining us today. I'm kind of glad that you brought up one of the topics as prevention of war because that's what this question is going to devolve to. War prevention is an ascendant topic these days. And along with the studies of war prevention have come a re-look at traditional concepts of deterrence and its relationship with escalation dominance. During the Cold War, the tightly scripted and controlled flow of information was an important part in the ability to effectively employ escalation dominance in a traditional geopolitical scenario.

What I'd like to know -- and this is a two-part question -- is, with the kind of integrated community that exists in cyberspace today and is projected to grow in the future, has this rendered the concept of escalation dominance moot by removing a primary means of control from the traditional nation states toolkit? And if not, then how do we manage it?

(Pause.)

MR. HOLT: And Colonel?

(Pause.)

Q Maybe he didn't like that question. (Laughs.

)

MR. HOLT: I think -- you know, I heard somebody drop off. I'm thinking maybe that it was they may have hit the wrong button here a minute ago.

Q I was going to ask him about getting stuff out timely. Boy, that takes care of that question. (Laughter.)

Q Way to manage your principal, Jack.

MR. HOLT: (Laughs.) Yeah, I knew I should have made another trip out there. We'll give it just a couple of minutes here, and they should be dialing back on.

There we go. This is Jack. Who is joining us?

COL. PARKS: Hey, Jack, this is Wayne Parks back. You know, we're so excited out here in Kansas because of the Jayhawks that we decided to take a little break there so we could come on again.

MR. HOLT: (Laughs.) Okay. All right, sir. Well, I'm guessing you probably didn't hear the question that the Steeljaw Scribe had just posed.

So Steeljaw, why don't we try this one more time?

Q Okay, thanks.

Colonel, war prevention is an ascendant topic these days. And along with the studies of war prevention have come a re-look at traditional concepts of deterrence and its relationship with escalation dominance. During the Cold War, the tightly scripted and controlled flow of information was an important part in the ability to employ escalation dominance in a traditional geopolitical scenario. What I'd like to know -- and this is a two-part question -- is, with the kind of integrated community that exists in cyberspace today and is projected to grow in the future, has this rendered the concept of escalation dominance moot by removing a primary means of control from the traditional nation states toolkit? And if not, then how do we manage it? COL. PARKS: Okay, you know, the one thing that we are attempting to do is understand that the environment, either in the past or now, probably hasn't been as easy to control as we might think it is. The idea of control may not necessarily be the right approach anyway. I know that what we're doing here at the Combined Arms Center is emphasizing the need to be able to take that risk that someone is going to say something that we may not be able to control. But at the same time, it's not to be worried about it because just being aware of what's being said and continuing to inform people and let them know the facts, I don't think that we're going to have any trouble.

What we have found, both in the cyberspace world and down on the ground where we can't control what the soldiers are saying a lot of times anyway, is they're saying the right things. And I think they're saying the right things because they believe in what they're doing and what we're doing is in our training is we're trying to emphasize to them the level of discipline that's necessary when you say something it has a tremendous amount of impact not only where you're operating in but depending on if you're in the cyberspace world or not, it gets out, and that has an impact overall.

So I think what we're finding is that that's not necessarily a problem for us nor are we looking to control this information. We're just looking to inform our folks well enough that when they say something, they are well informed and they're going to state the facts and they're going to state, you know, the real reasons why we're doing what we're doing. I'm not too concerned about the idea of cyberspace and control of cyberspace, or on the ground or control of what out folks are saying on the ground. It's just a matter of good information and well informed soldiers and leaders.

Q So to sort of follow up on that, then, if we step outside of just looking at our own forces and look at the issue of the message and how it may or may not be perverted by outside non-state actors, for example, how do you address that?

COL. PARKS: Well let me make sure I understand your question correctly is is that the idea is someone -- a non-state actor is saying something that impacts what we're doing or not doing? Now, again as is obvious, they're not speaking for us, so I'm not too worried about that. But the fact that we're able to know what's being said, and we're able to be the -- proactively or reactively deal with that by putting our own information out and making sure we stay -- either stay ahead of the game or we are able to react to what's being said. Again is -- we should be okay; we should be okay without having to ever worry about controlling what everybody is saying. We just need to get our own story out, get our own messages out, and I think we have learned over time, as

in especially the United States Army, we've learned over time is -- is there's a lot of respect for what we do and that ends up doing the job for us.

Q Okay, thank you. MR. HOLT: All right, Andrew.

Q Colonel, good morning, Andrew Lubin from the Military Observer. I appreciate you taking the time to speak with us.

Sir, I -- looking at the PowerPoint you sent out yesterday -- and I'm on page 5, Implications and Conclusions -- and I'm looking at the part that talks about dividing what audiences -- enemy, adversary, friendly or neutral, et cetera. Then you finish up by saying the ultimate goal must be to synchronize the operations of our -- to our messages. Doesn't that ring -- take what you're doing, which is pretty much a reactive and -- (audio interference) -- action -- Jack, is he still on?

COL. PARKS: I'm still here.

MR. HOLT: Yeah.

Q Oh good, thanks. It seems to me you take -- I mean cyberspace is quick to respond, today in an hour, maybe five minutes ago, and you've got to turn around and get different people signing off on things and rewriting it -- you dumb it down, and you end up with either a Jessica Lynch or Pat Tillman type of problem, or you're two weeks out of date by the time things are posted on the web. Or am I misreading this? COL. PARKS: Jack (sic), you're trying to find the PowerPoint slide you say we sent out yesterday, and I'm not sure I've got the same slide here. We put out some information papers one through four that talk --

Q This is on page -- let me dial it back for you, sir. It's Paper Number Two, Information on Cyberspace Issue around line number 118. COL. PARKS: Okay.

Q I'm not trying to trick you up, I just want to make sure that we're all on the same page on this, so to speak.

COL. PARKS: Yeah.

You know and again if I understood your questions - your question correctly is I think I heard you say that we have a tendency of being reactive, and I agree with you is 00 is we do have a tendency of being very reactive. Our intent is, though, is with the idea of information in cyberspace is to get on the proactive side of this -- you know, being able to put the messages out in advance and putting the word out in advance of what we're doing versus continually finding us in a reactive mode. Now, of course, we'll never be able to avoid that idea thatsomeone's going to say something and we're going to have to respond to that. Q But if you do --

COL. PARKS: But the luck we have on putting our information engagement construct together is we bring the right people together, working together to be able to stay ahead of that game. Does that answer your question, or did I misread your question?

Q No, it was pretty good. But let me follow up on that, please, Jack, because you said we have time --

MR. HOLT: Yeah.

Q But, sir, then you -- you look at the situation, it almost strikes me like you don't trust your own soldiers. If somebody says something wrong, so what? General Manus of the Marine Corps was recorded and actually still bothered about it, talked about shooting some Afghan men because he said they fight like women anyway. You know, what's wrong -- if somebody makes mistakes, so what?

(Cross talk.)

COL. PARKS: Yeah, you actually -- you actually get that --

(Cross talk.)

COL. PARKS: -- to the way the Chief Staff of the Army and -- actually General Wallace and General Caldwell are trying to impress upon everybody is is that we should not worry about what's being said, because, again, our folks are saying the right thing.

I mean, 80 percent of the time -- and I'll just throw a number on it -- you know 80 percent of the time that they're saying the right thing, take a little risk with that 20 percent of the time that they may not say exactly what it is that you want them to. But at the same time, as long as you're aware of what's being said, you can always correct the record or you can always inform people, adequately, to ensure that we, again, don't stay on this reactive mode and don't look at our soldiers and our leaders out there and mistrust them, let's trust them exactly as you describe.

General Caldwell has got us out here talking to you folks because he is not worried about what I'm saying to you today, nor should he. Nor am I worried about the soldier or the specialist or the corporal down there on what he's saying because if I'm keeping them properly informed, they're going to say the right things that are going to help our cause.

Q Okay, great, thank you.

MR. HOLT: Okay, David.

Q Hi Colonel. It's David Axe from War is Boring. Okay, so I read through the documents that Jack sent us and took a look at the PowerPoint and I think I get some of the cyberspace information control thing, but I'm really confused, which is funny, because the stuff Jack sent us spent its first half trying to explain what information is, and I don't get it. So maybe you can explain it to me where's the overlap between intelligence and information? And I want to follow up on that.

COL. PARKS: Well, I'm an old Calvary soldier and trooper, and I would tell you is I don't see the difference between intelligence and information because as I've used intelligence over my career, that's exactly what it's been -- it's been information about the environment I'm operating in. So to a large degree as I equate what I get from the intelligence community as being the information I need to operate with.

Q So, what's new here?

COL. PARKS: Well, the -- I think what's new is maybe the medium that we're operating through. Because I've seen a chart here recently you know there was a day when we were operating at foot speed, we move to wheel speed, we got into air and we move to air speed, and now we're talking about moving at computer speed or cyber speed. So what really is changing for us now is how rapidly information is moving around the battlefield and how rapidly the enemy can use the information and that we have to be able to pick up the pace differently than we have in the past. We have to be able to respond, react, be proactive enough to stay out ahead of the speed of megabytes. I think that's the major difference of what we've seen in the past and what we're seeing now we're certainly going to see in the future.

Q But we're not talking about fundamental changes in the way in the Army's attitude and the way it operates. I mean, so -- okay, so things are faster but they aren't different other than being quicker. Fundamentally, the way that the Army deals with intelligence both receiving and interpreting it and broadcasting it for another customer, so to speak. It's the same, fundamentally. It's just faster, right?

COL. PARKS: Yeah. I would say that that's true. Because, again, is the information on the environment -- and I say environment because as you all know our intelligence is just not about the enemy, it's about the operating environment that they're working with as well. And I think that the main difference that we are talking about is just speed. And how the Army's going to handle that is going to have to be to find a way to maneuver around what the enemy's doing a lot faster than we've done in the past. You can kind of equate it to the vignette I gave you a second ago is -- is you know, we've had to do that on a number of occasions, especially in the last century where it's really been speed that's made a difference, and we've had to end up finding a way to do things faster than we have in the past, and be able to -- actually staying ahead and proactive is probably the biggest change.

But I don't know that I could give you specifics on those fundamental changes yet. I would tell you that the symposium we're running next week -- it's called an Information in Cyberspace Symposium -- we're tackling an issue just like that, trying to determine what is fundamentally different across the functions we currently perform because of the way information is being used and the different mediums that information is coming across today.

So I may not be able to answer that question today, but what I hope to be able to do for you several months down the road is to give you a better answer to your question.

Q Okay. Thanks.

MR. HOLT: All right. Looking forward to that.

Bruce.

Q Hey, Colonel. Bruce McQuain with QandO.net. A lot of this is obviously theoretical. We're talking information flow, information protection -- that type thing. I'm more interested in stuff like the Chinese and what they're doing as far as what seems to be a fairly sophisticated and big information operation -- cyberspace, whatever you want to call it -- capability to attack us. How do we address that?

COL. PARKS: Well, and I think again, from an Army perspective, is that we don't necessarily know how we're going to answer that yet.

You see the commercials coming on TV with the Air Force, you know, and they're trying to commit a significant amount of resources towards their definition of cyberspace. And what the Army and the Marine Corps and the Navy are doing, as well, is is all trying to get together and determine how we are going to address major -- a larger threat than what we see now.

You know, what we're getting off the battlefield now is things like we're using electronic warfare capabilities in defeat of the improvised explosive devices. We're also using computers, networks, electronics in order to be able to engage the enemy on websites -- on their websites -- and being able to, again as we talked before, to get the message out either before the enemy gets the message out or be able to respond to the enemy as they're putting the message out.

That's a fairly low threat, compared to what you just described. And I would say China and Russia -- and I'd name those two countries now who probably have a tremendous amount of capability in the area of what we're defining as cyberspace to both attack, defend and exploit here in the near term.

And so what we've done here is stood the proponent up five months ago -- seven months ago now -- for computer network operations and electronic warfare to answer that full-spectrum operation question, one of which is on the far end that you just described. And of course, the other to deal with the immediate threats that we're dealing with across the globe at a smaller level.

Q Appreciate it.

MR. HOLT: Okay.

And John.

Q Good morning, Colonel, "Leavenworth's Tame Outside the Gate" blogger here.

The thing I find interesting about this is I'm in an odd position -- and we'll make this very "bloggy", because this will be feedback as much as it is -- more than it is a question. I found myself in demand on the fort just yesterday. I was talking to Mark Forman and his guys at the battle lab. And they're trying their best to implement General Caldwell's guidance to get out and tell the stories and do that kind of stuff, but they're also very wary of doing it wrong. And the things you said, you know, take the risk and step back and trust them.

And one of the -- one of the first IOs was in that meeting and I can't remember his name right now, but the tension between the two was -- and I don't mean this in a negative way -- but was palpable between the two viewpoints on what to do and how to do it.

And I was wondering how we're going to go about trying to, because the young troops clearly -- they got it. They know what they want to do. The problem -- just like in public affairs with getting the message out -- the problem is residing at the lieutenant colonel- colonel level and getting them to understand how things work now. And what, if anything, we're going to try and

do -- just wait for those guys to retire or find ways to kick them off the top dead center?

COL. PARKS: Yeah, that's a good point.

You know, I walked in here in the end of August and the first thing I told my crew for CNO and electronic warfare, I looked around and saw we had a bunch of active or retired lieutenant colonels probably 45 years and older. And the first thing I ordered was change the demographics. Find the new generation, bring them in here and let's start listening to them and let's start taking what they're saying versus what we know.

And then, of course, obviously take our experience in military operations and be able to learn from them and then use that in what we think would be best for military operations.

And we're actually having some success with that. I'm starting to see folks come out that are in their mid to late 20s -- that's good. We have gone out to the local schools here and we've taken a look at some of the teenagers and just talked to them. Interestingly enough, how much they know about hacking, and how much they know about what we professionally describe as computer network attack and computer network protect.

We've gone to the universities here within the big 12 -- probably about three of them now -- and we're looking to expand that. And we're talking to them, because I want to learn from that new generation that's coming up through the college and the education system and have them teach us not only about the hard sciences, but about the soft sciences as well, because they have a different way of doing things.

But it's the real world that we're operating in today that many times us lieutenant colonels and colonels -- those of us that are over 40 years old -- just can't get yet. And it's not a statement about our leadership. Our leadership is strong. It's just the leadership needs to recognize is that what we want to do is get that new generation engaged here. And we're doing that at the Combined Arms Center.

Going back to the universities, you know, we're going out to the universities and I've asked them for help in a couple of areas. One is the area of humanities and social sciences. That gets toward this information engagement thing that I told you about earlier. And the other side is that the natural sciences and the formal sciences -- we start getting at some of the technological and electromagnetic spectrum type -- the understanding of those things as we're making these decisions and developing capability within Combined Arms Center.

We've got to understand that in a different light than what guys like you and I have understood that in the past. So we're making a very concerted effort there -- at least down in these two proponents down here at the back side of the prison -- the old prison in the old stables.

Q (Laughs.) All right.

Sorry about that little giggle. I worked in that building once when it was a war gaming center. Thank you, sir. Appreciate it.

COL. PARKS: You're welcome.

MR. HOLT: All right. Griff.

Q Hey, Colonel. Thanks for joining. Griff Jenkins, Fox News.

I want to follow up a little bit on Bruce. Bruce's question got me very interested. And we read a lot about China's domination and so this is, I guess, a general question -- hopefully you can shed some light on it and give me a more concrete answer.

Do you -- are we in -- for those that don't understand so much as even your title, Colonel, which would be myself -- the simpletons out there -- are we in an electronic war with China and Russia right now? And are you being attacked? Are there -- is there a -- are you getting computer attacks? Are you trying to control the CNO concepts out there against China? What can you say about that?

COL. PARKS: Well, you know, first of all is having grown up in the Cold War and started my career there, you know, there was always the big bear on the other side. And I think we always thought that they were much bigger and badder than what they really ended up being.

The one thing we don't want to do is put ourselves in a position that, you know, China and Russia are so big and bad in this area that we within the United States are not doing a good job, nor we can't do a good job to be able to either defend ourselves or to operate in that same environment as them.

From an unclassified perspective, I think across the United States you can go read anywhere that there are attacks being made on our networks and our computer systems -- whether it be hardware or software from across the globe. And so we're very aware of that.

We're trying to learn more about what that really means, you know, how bad is it? I don't know that I could answer that and even if I could, I probably couldn't do it in this forum.

We at the Combined Arms Center are learning from that and building capabilities which allow us to operate and defend ourselves against any type of attack that may be coming from the sources that I mentioned earlier -- China and Russia.

So yes, we are engaged in it. Yes, we are building capabilities to be able to deal with it. And that's both in what I'm calling computer network operations and electronic warfare. One you could almost equate to being a wired method, the other is a wireless method -- and that's the way a lot of people try to describe it to you.

As I mentioned earlier, just the iPhone alone, you know, puts a computer in my hands. It puts a network which actually goes across the electromagnetic spectrum or the wireless environment. And there's more and more of that going on than there is just coming through wires across the ground.

I mean, space capabilities -- shooting a signal up to a space satellite and then back down to the earth. A tremendous amount of what we're talking about here is going through that environment. So to a large degree, is yeah, the answer to your question is yes.

MORE Question: Greg Rand (sp), Mexico - that's how I heard one of the questioners identify himself. there's more and more of that going on than there is just coming through wires across the ground. And in space capabilities, shooting a signal up to space satellite and then back down to the earth -- a tremendous amount of what we're talking about here is going through that environment.

So to a large degree, the answer to your question is yes, we do feel, within the electromagnetic environment and within the computer network environment, whether it's wired or wireless, there's a tremendous amount of attacks. And we're building capability and we're dealing with that now within the United States.

Q Great. And I guess just a follow-up that may or may not actually make ties. Are you learning things as you operate within theater in Iraq and Afghanistan? Are there lessons learned there that will translate to this larger war with these other players?

COL. PARKS: Yes. The other day we were talking about that. In both Afghanistan and Iraq, we're learning a tremendous amount. We do a lot of work on lessons learned and best practices. We have an office here in Fort Leavenworth called the Center for Army Lessons Learned, and they're linked in to several different lessons learned forums and websites where we pull in from our multinational partners and the other services many of the lessons learned.

We're doing a thing called best practices where we go talk to the folks as they come back from theater or while they're in theater to understand how they're doing things and how they're dealing with these types of issues.

The one thing that we don't want to forget, though, is that's just two places in the world. And the way things are being done in those two places are not necessarily the same as some other places across the world that are happening, such as we're engaged in South America, we're engaged in the Philippines, we're engaged in those other portions of the world. And then, of course, as we just discussed, you've got, like China and Russia, you know, which is a very global reach and not necessarily a regional reach.

But, yes, we are learning from those two operating environments. But at the same time, that's being combined with what we're learning across the rest of the world as well.

Q Thank you.

MR. HOLT: All right.

Anyone else joined us?

Q Yeah, this is Greg Rand (sp), Mexico.

MR. HOLT: Okay, Greg.

Q Hey, Colonel, I'm doing some work on this whole notion of the animated decision loop and decentralized enemies such as some people have labeled Hezbollah a hybrid enemy. I just wanted to know if you have examined how you do get into an enemy's decision loop who is highly decentralized into smaller cells and such, who doesn't have that kind of hierarchical command structure that western military has. Is that something you're looking at?

COL. PARKS: Yes. As a matter of fact, as you well know, in the cyber world, or electronic world that we're in now, that creates those types of environments and those types of decision-making processes. And actually you almost can't call them processes in some cases.

It's opportunistic in a lot of ways. And, yes, we're taking a very hard look at how folks are operating across the globe within the different regions where they're not a very well-structured or hierarchical type organization the way you and I know it.

I was talking to some folks the other day about when a thing called Red Hat, you know, was being developed out on the Web and how it was just a matter -- a good idea was tossed out there and then three or four more good ideas came back, and they started collaborating on that good idea. And then that good idea got tossed out and maybe five or six other folks, and exponentially this started playing out to where they were building software just out of a collaborative group that was not any sort of a corporation or structured hierarchical organization. And, of course, that's certainly what our enemies are doing to us now.

So, yeah, we're spending a lot of time trying to figure out how do you define that environment and how do you then get in the environment to be able to either disrupt, destroy, defend, or whatever the case may be, those types of decision-making capabilities.

Q So you think a decentralized enemy still has that OODA loop notion that Boyd made famous, something you can intercept or embed yourself in somehow?

COL. PARKS: Yeah, that's a good question. I'm not sure I could answer. I mean, I wouldn't necessarily compare it to something as strict as an OODA loop. I mean, some people would say maybe it's not quite as strict a process as I make it sound, but there is going to be places of weaknesses out there even with these distributive type of decision-making or distributive type of sharing of information.

And what we're going to have to do is we're going to have to find a way to go after those weaknesses at the same time as being able to understand where the strengths are. But I think there is something that is structured when you really get down to the final analysis that you can actually get at.

Q Okay, thank you.

MR. HOLT: Okay. Anyone else? Okay, any follow-up questions?

Q Jack, this is Steeljaw. I've got one quick one.

MR. HOLT: Sure.

Q Yes, Colonel, you touched on this a little bit earlier when you mentioned the partnership with the Marine Corps. And the question is, as you proceed on this path, how do you go about making sure that you integrate well with other services, agencies and organizations, particularly outside of DOD, so that everybody doesn't end up working at cross-purposes? What do you see as the biggest challenges in that?

COL. PARKS: Well, first, with the Marine Corps, it's pretty simple. We both operate in pretty much the same environment, which is why we've got to make sure, from the land component perspective, we're tight with our Marine Corps partners. At the same time, it's pretty automatic when you start talking about -- we do operate land, sea and air pretty much between the Marine Corps and the Army, and so it's a natural tendency to go to your Air Force and your Navy partners and work and collaborate with them.

The biggest challenge is what I mentioned in the opening statement is that there's a tendency to wait until each service has an approval or an approved answer to something and then start working together. What we're doing is we want to break that down and say, "Hey, I'm starting from the beginning, as I'm coming up with the idea, the concept, the doctrine from the initial stages, I'm sitting down with my joint partners and we're writing this collaboratively," versus writing this as individuals. That's not as hard to do within the joint services within the United States.

I just spent yesterday and today, when I go to the multinational aspect, is with some of our multinational partners as well. And over the last four weeks -- (inaudible) -- have spent a lot of time collaborating with them on what we're doing in information engagement, computer network operations and electronic warfare. And that also doesn't seem to be that difficult when we're working military to military.

The challenge comes is the trust between the interagencies and the different governmental organizations. And what we have to do is like we're doing now. We're starting to invite them to the table as well. General Caldwell, for example, spends quite a bit of time bringing our interagency and intergovernmental partners out here to Fort Leavenworth and making them part of our symposiums and conferences, starting to invite them to be part of our education system, providing seats in the different courses out here.

But the challenge is overcoming their ability to send somebody from a job they're doing within their organization and spare them for the education that we want to give them or for the conference or the symposium we want to have them at; at the same time is to break down those barriers of trust between the different governmental agencies on what we're doing. So those are probably the biggest challenges I see right now that we're spending a lot of time under General Caldwell trying to overcome.

Q Okay, thank you.

MR. HOLT: Okay, anything else? Anyone else?

Q Jack, I have one.

MR. HOLT: Okay, go ahead.

Q Colonel, Andrew Lubin from the Military Observer.

Sir, if we're fighting, and we'll probably continue to fight non-traditional enemies, is it possible, instead of trying to have one unified voice that takes a lot of time to get something set up like that, where you let the troops on the ground, the commanders on the ground, have some local authority?

For example, last week, when Basra was all erupting and not doing well, we sent some e-mails over asking for some information. (Inaudible) -- back two days later was a press release out of MNF-I Central talking about a basketball clinic that lasted two days; not a timely nor interesting response. How are you going to win the information war when that's what comes back?

COL. PARKS: You bring up a good point. And we aren't doing a very good job on that. Soldier-leader engagement in terms of how we're portraying information engagement in our doctrine should put us in a position to where a soldier or a leader gets engaged, then someone needs some information and they're able to respond immediately with the information. And, yeah, we're not as good as we could be.

I would tell you we have an intent to try to improve our structure to be able to allow that. As we talked a second ago, the speed of travel no longer is 15 hours to get across the oceans. The speed of travel is just, you know, milliseconds when, for example, you probably sent that in an e-mail form, I think I heard you say, and certainly somebody could respond in an e-mail fairly quickly.

We have to get ahead of that game. We're not as good as we should be, but hopefully the construct that we're putting together now with information engagement to emphasize leader and soldier engagement will start improving.

Q Okay, thank you.

MR. HOLT: Okay.

Q It's Griff with Fox. I apologize. Now you've got me thinking again about China and Russia and a little bit on Andrew's question. Are there other things that inhibit you? Are there rules of engagement problems, hurdles, challenges, that you have in competing at this -- responding or being proactive in trying to stay at that high speed and fend off attacks and also create our own advantages? Are there actual rules of engagement hurdles you face every day?

COL. PARKS: Yeah. You know, we put ourselves on the ground in the sea and in the air now. There are rules and policies and laws and so forth that limit our -- or at least govern the way that we deal with those air-land-sea and even space environments.

The one thing, obviously, in the Internet and the networks, those lines don't exist, and there's a tremendous amount of void in being able to have that law that governs. And we could take advantage of the law, but at the same time, maybe the law is not going to do it, either.

You mentioned rules of engagement. We in the military actually are pretty good in describing our rules of engagement to ensure we're doing the right thing. And we've talked here, in the last several months, on how would we in the military describe the rules of engagement we would operate under, which hopefully then would help describe the policies and the regulations and the laws that need to be written in order to support us being able to defend whatever it is we're trying to defend. In this case, obviously, we're signed up to defend the Constitution of the United States and what that means.

So yeah, we're a little bit limited because some of the policies and laws haven't caught up with the technology; they haven't caught up with the times.

But however, though, is we're trying to build those rules of engagement that allow us to operate and do what it is that the nation's asking us to do in defending our Constitution.

Q Thank you.

Q Colonel, Andrew Lubin again. But to follow up on Griff's question, but the Marine Corps can do it; why can't the Army? They've got the same --

COL. PARKS: You'd have to describe for me what the Marine Corps is doing.

Q Well, I can turn around and send an e-mail out to the people at RCT-5 or some -- al-Asad around Anbar, at Ramadi. I get a response within -- if it's an hour, I'm surprised. Or they run information. If I ask a question, I get a competent, qualified response on a timely basis. They don't need to -- they don't seem to have to have a consensus of general officers and -- (inaudible) -- officers to respond.

COL. PARKS: Andrew, you got me there. And you bring up a good point. If the Marine Corps is doing that very well, there's certainly a place we could go to to learn.

As I mentioned before, we'll talk to our Marine Corps partners and find out what they're doing that's better than what we're doing, and we'll see if we can't incorporate a little bit of that, both in the culture and in the processes for the United States Army.

Q Okay. Thank you.

MR. HOLT: Okay. All right, anything else? Anyone else?

Q Yeah, I've got one, Jack. This is John Donovan. One, Jack, you should be taking notes, because a lot of this stuff directly impinges on you and how your guys, the P.A., does business.

One of the things I noticed, Colonel Parks, is I've had Andrew Lubin's issues about trying to get -- getting into MNFC-I, et cetera, depending on which e-mail I'm using. And that might be a problem that Andrew has; I don't know. Q John, they just don't respond. I followed up with a phone call.

Q Oh, okay.

(Cross talk.)

Q They came back with -- again, useless information about a basketball -- (audio interference) -- instead of -- as Basra's going to pieces.

Q Okay. But my point being is when I try to get in contact with guys in Afghanistan, nothing ever goes through unless I use my AKO address, which is obviously an unfair advantage I have as an Army retiree. Then if I do it, if I get the sergeant specials answering, it all comes back pretty quick. But again, it comes back -- something else Andrew said. If I'm dealing with the majors and above -- it goes back to our own internal corporate culture in the service -- it comes back bland and pointless.

COL. PARKS: And, you know, there is something that General Caldwell also did when he first came on board. We have now got this idea of information engagement, and probably less on the CNO and electronic warfare, even though we're working very rapidly to try to incorporate that into our leaders' courses.

And Fort Leavenworth's a great place to do that from, because we have most of the leaders come through here, in one form or fashion or another. But through the Command and General Staff College, through the pre-command course, other senior leader courses and the leader development office here within Fort Leavenworth, he has expended an inordinate amount of his time and our time on ensuring those leaders come through and we talk to them about this.

You know, we may be in a generational thing that we're seeing some folks are going down-range and they're immediately responding to that, reacting to that, and doing a pretty good job. There are others that are coming through here and maybe not being able -- they may be -- their culture may be such that they're still living the Army dream, here, and are a little concerned about taking that risk of answering your question. Because in some cases, we in the Army, over the past many years, have not done a good job in trusting when somebody asks us a question.

You'll find that the answers now should be on point and they should be to exactly what you're asking. I don't feel the least bit worried about answering your question, as long as I keep the security where it needs to be, and giving you the best answer I can to specifically answer your question instead of, like you're saying, give you some bland answer that really doesn't get at the point that you're asking the question on.

Q Thank you, sir.

MR. HOLT: All right. Okay, looks like we've got, across the board, a lot to learn.

COL. PARKS: We have.

MR. HOLT: We've just to stay engaged. So, Colonel, I appreciate your being with us this afternoon -- or, this morning. And hopefully we can re-address this, perhaps after your symposium coming up next week.

COL. PARKS: Gentlemen, again, I thank you for your patience with me and tolerance of me. I hope I've done a good answering your questions. I'd hate to find out later that I gave you a bland answer to a specific question you asked.

But certainly, please give us that feedback, and if I've not done as good a job as I could, I'll improve on that. And we'll certainly be looking forward to coming back and speaking with you at a later date, if we can. Because, again, I'm thinking it's going to be about a month to two months here for us to frame where the Army needs to go with this idea of information engagement, cyber- and electronic warfare. And I'd be glad to join back with you and hopefully show you some progress on where the Army's at.

MR. HOLT: All right, sir. I think we can do that. We'll be here, and we look forward to it as we move towards moving at the speed of thought.

Colonel Wayne Parks, director of the Computer Network Operations Proponent, Electronic Warfare Proponent, and also TRADOC capabilities manager for electronic warfare integration at the Combined Arms Center at Fort Leavenworth.

Thank you very much for joining us today, sir.

COL. PARKS: Thank you, Jack.

Q Colonel, thanks for the time today.

Q Thanks, Colonel.

COL. PARKS: You bet, gentlemen.

Q Thanks, Colonel.

COL. PARKS: Colonel Parks out.

END.